



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 4月 2日

出 願 番 号

Application Number:

特願2001-103058

出 願 人

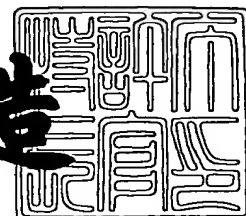
Applicant(s):

日本電信電話株式会社

2001年 6月13日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3055436

【書類名】 特許願

【整理番号】 NTTH127203

【提出日】 平成13年 4月 2日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/62

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 斎藤 賢一

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 重松 智志

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 町田 克之

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 首藤 啓樹

【発明者】

    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

    【氏名】 足立 卓也

【特許出願人】

    【識別番号】 000004226

    【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100064621

【弁理士】

【氏名又は名称】 山川 政樹

【電話番号】 03-3580-0961

【手数料の表示】

【予納台帳番号】 006194

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701512

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ゲート開閉システム

【特許請求の範囲】

【請求項 1】 会場の入場ゲートを開閉するゲート開閉システムにおいて、  
利用者の生体情報に基づき利用者本人を認証する認証トークンと、  
利用者が前記会場の入場料の前払いを行うと前記利用者の識別情報が記憶されるデータベースと、

利用者の前記会場への入場時に前記認証トークンにより前記利用者が本人であると認証されこの認証トークンに予め記憶されている前記利用者の識別情報が前記認証トークンから出力されると、この識別情報を受信するとともに受信した識別情報が前記データベース内に記憶されている場合は前記入場ゲートを開放する制御手段と

を有することを特徴とするゲート開閉システム。

【請求項 2】 会場の入場ゲートを開閉するゲート開閉システムにおいて、  
利用者の識別情報が記憶される認証トークンと情報の授受を行う情報授受手段と、

利用者が前記会場の入場料の前払いを行うと前記利用者の識別情報が記憶されるデータベースと、

利用者の前記会場への入場時に前記利用者の生体情報に基づき前記認証トークンにより利用者本人であると認証されこの認証トークンから出力される利用者の識別情報が前記情報授受手段により受信されると、この受信識別情報が前記データベース内に記憶されている場合は前記入場ゲートを開放する制御手段と

を有することを特徴とするゲート開閉システム。

【請求項 3】 請求項 1 または 2 において、  
前記認証トークンは、利用者の指紋情報に基づき利用者本人を認証する指紋認証トークンであって、

利用者の指紋情報を記憶する記憶手段と、

利用者の指紋を検出する指紋センサと、

前記指紋センサの検出情報と前記記憶手段の記憶情報との一致に基づき前記利

用者を本人と認証する処理手段と

を有することを特徴とするゲート開閉システム。

【請求項 4】 請求項 3 において、

前記指紋認証トークンが挿入され、かつ利用者が前記会場の入場料の前払いを行うと、パスワードを生成して生成したこのパスワードを前記指紋認証トークンに前記識別情報として記憶させるとともに、前記データベースに送信して前記利用者の識別情報として記憶させる識別情報付与手段を備えたことを特徴とするゲート開閉システム。

【請求項 5】 請求項 3 において、

前記指紋認証トークンには予め利用者の識別番号が前記識別情報として記憶され、

前記指紋認証トークンが挿入され、かつ利用者が前記会場の入場料の前払いを行うと、前記指紋認証トークンの識別情報を読み取って前記データベースに送信し前記利用者の識別情報として記憶させる識別情報付与手段を備えたことを特徴とするゲート開閉システム。

【請求項 6】 請求項 1 ないし 5 の何れかにおいて、

前記認証トークンに付加されこの認証トークンから出力される識別情報を無線信号または赤外線信号に変換して送信する送信手段と、

前記入場ゲートの近傍に配設され前記送信手段により送信される無線信号または赤外線信号を受信すると、受信した無線信号または赤外線信号に含まれる前記識別情報を前記制御手段に送出する受信手段と

を備えたことを特徴とするゲート開閉システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンサート会場や競技場の入場ゲートの開閉を行うゲート開閉システムに関する。

【0002】

【従来の技術】

コンサート会場で催される所望のコンサートを聴く場合、利用者は予め該当するコンサートのチケットを購入し、コンサート開演前にその会場のゲート近傍の係員にそのチケットを手渡すとともに、係員がそのチケットをチェックすることにより利用者のコンサート会場への入場を許可するようにしている。

また、例えばサッカー競技場で行われるサッカーの試合を見物する場合も、利用者は同様に予めチケットを購入し、試合開始前にその競技場のゲート近傍の係員にそのチケットを手渡すとともに、係員がそのチケットをチェックすることにより利用者の競技場への入場を許可するようにしている。

#### 【0003】

##### 【発明が解決しようとする課題】

しかしながら、こうしたコンサート会場や競技場への入場時に係員がチケットをチェックする方法では、チケットのチェックに多くの係員が必要になるとともに、利用者がコンサート会場や競技場への入場するのに長時間を要するという問題があった。また、利用者のチケットが盗難に遭った場合、そのチケットを利用した第三者による会場への不正入場が行われてしまうという問題もあった。

#### 【0004】

したがって、本発明は、利用者のコンサート会場や競技場への入場の際にチケットのチェックを行う係員を要することなくかつ利用者の速やかな入場を可能にするとともに、コンサート会場や競技場への第三者による不正な入場を阻止することを目的とする。

#### 【0005】

##### 【課題を解決するための手段】

このような課題を解決するために本発明は、会場の入場ゲートを開閉するゲート開閉システムにおいて、利用者の生体情報に基づき利用者本人を認証する認証トークンと、利用者が前記会場の入場料の前払いを行うと利用者の識別情報が記憶されるデータベースと、利用者の前記会場への入場時に認証トークンにより利用者が本人であると認証されこの認証トークンに予め記憶されている利用者の識別情報が認証トークンから出力されると、この識別情報を受信するとともに受信した識別情報がデータベース内に記憶されている場合は入場ゲートを開放する制

御手段とを備えるようにしたものである。

この場合、認証トークンを、利用者の指紋情報を記憶する記憶手段と、利用者の指紋を検出する指紋センサと、指紋センサの検出情報と記憶手段の記憶情報との一致に基づき前記利用者を本人と認証する処理手段とからなる指紋認証トークンにより構成したものである。

#### 【 0 0 0 6 】

また、本システムは、指紋認証トークンが挿入され、かつ利用者が前記会場の入場料の前払いを行うと、パスワードを生成して生成したこのパスワードを指紋認証トークンに識別情報として記憶するとともに、データベースに送信して利用者の識別情報として記憶させる識別情報付与手段を設けたものである。

また、本システムは、指紋認証トークンに予め利用者の識別番号を識別情報として記憶し、かつ指紋認証トークンが挿入され、利用者が前記会場の入場料の前払いを行うと、指紋認証トークンの識別情報を読み取ってデータベースに送信し利用者の識別情報として記憶させる識別情報付与手段を設けたものである。

また、本システムは、認証トークンに付加されこの認証トークンから出力される識別情報を無線信号または赤外線信号に変換して送信する送信手段と、入場ゲートの近傍に配設され送信手段により送信される無線信号または赤外線信号を受信すると、受信した無線信号または赤外線信号に含まれる識別情報を制御手段に送出する受信手段とを設けたものである。

#### 【 0 0 0 7 】

##### 【発明の実施の形態】

以下、本発明について図面を参照して説明する。

図 1 は、本発明に係るゲート開閉システムの構成を示すブロック図であり、本システムは、コンサート会場や競技場に設けられたゲートの開閉を行うものである。

#### 【 0 0 0 8 】

図 1 において、本システムは、チケット販売店及び利用者の自宅に設けられ後述の指紋認証トークンが挿入され利用者がチケット代金を支払うとパスワード等を発生して指紋認証トークンに保存させるクレードル 1 0 1 と、クレードル 1 0

1とネットワーク105を介して接続されたデータベース102と、データベース102に接続されるとともに、コンサート会場や競技場に設けられたゲート104近傍に配置されゲート104の開閉を制御するゲートコントローラ103と、前述の指紋認証トークン106と、無線通信ユニット107と、赤外線通信ユニット108と、ゲート104の近傍に配置され無線通信ユニット107または赤外線通信ユニット108からの信号を受信してゲートコントローラ103に出力する無線／赤外線信号受信装置109とからなる。

#### 【0009】

前記クレードル101に差し込まれる指紋認証トークン106は、利用者が所持し、持ち運びのできる小型、軽量の装置であって、図2に示すように、本体部201が設けられているとともに、本体部201に、指紋センサ202と、処理装置203と、記憶装置204と、クレードル101との接続端子である端子205とが設けられている。そして、処理装置203は、指紋センサ202、記憶装置204及び端子205に接続されている。

#### 【0010】

また、前記無線通信ユニット107は、図3に示すように、指紋認証トークン106にアダプタ301を接続したものである。アダプタ301内には指紋認証トークン106の処理装置203と端子205を介して接続され処理装置203の出力信号を無線信号に変換する無線信号発生回路303が設けられ、この無線信号発生回路303とアンテナ302が接続される。

#### 【0011】

また、前記赤外線通信ユニット108は、図4に示すように、指紋認証トークン106にアダプタ401を接続したものである。アダプタ401内には指紋認証トークン106の処理装置203と端子205を介して接続され処理装置203の出力信号を赤外線信号に変換する赤外線信号発生回路403が設けられ、この赤外線信号発生回路403と赤外線光源402が接続される。

#### 【0012】

図12は前記指紋認証トークン106を構成する指紋センサ202の概略的な断面を示す図である。本指紋センサ202は、例えばシリコンからなる半導体基



板 2 1 1 上の下層絶縁膜 2 1 2 上に形成された層間絶縁膜 2 1 4 上に、たとえば  $80\ \mu\text{m}$  角の複数のセンサ電極 2 1 5 と、格子状のアース電極 2 1 6 とを備え、複数のセンサ電極 2 1 5 とアース電極 2 1 6 とを、層間絶縁膜 2 1 4 表面で規定される同一平面上に配置している。

## 【 0 0 1 3 】

センサ電極 2 1 5 は、層間絶縁膜 2 1 4 上に形成されたパシベーション膜 2 1 7 で覆い、 $150\ \mu\text{m}$  間隔に複数個を備えるようにするとともに、Au から構成し、膜厚  $1\ \mu\text{m}$  程度に形成している。パシベーション膜 2 1 7 の膜厚は  $3\ \mu\text{m}$  程度としたので、センサ電極 2 1 5 上には、パシベーション膜 2 1 7 が約  $2 (= 3 - 1)\ \mu\text{m}$  存在している。このパシベーション膜 2 1 7 は、例えばポリイミドなどの比誘電率が 4.0 程度の絶縁物から構成される。

## 【 0 0 1 4 】

上記下層絶縁膜 2 1 2 上には、センサ電極 2 1 5 にスルーホールを介して接続する配線 2 1 3 を形成する一方、半導体基板 2 1 1 上には、センサ電極 2 1 5 に形成される容量を検出する容量検出回路 2 1 8 を形成している。この容量検出回路 2 1 8 は、前述した配線 2 1 3 によってセンサ電極 2 1 5 に接続される。容量検出回路 2 1 8 は、センサ電極 2 1 5 毎に用意され、センサ電極 2 1 5 と認識対象（指）の一部との間に形成される容量を検出する。

## 【 0 0 1 5 】

各容量検出回路 2 1 8 の出力は、処理装置 2 0 3 に接続され、この処理装置 2 0 3 により、各センサ電極 2 1 5 に形成された容量を濃淡に変換した指紋画像データが生成される。

各容量検出回路 2 1 8、処理装置 2 0 3 及び記憶装置 2 0 4 は、たとえばセンサ電極 2 1 5 下の半導体基板 2 1 1 上に形成する。これにより指紋センサ 2 0 2、処理装置 2 0 3 及び記憶装置 2 0 4 をワンチップ化でき、したがって指紋認証トークン 2 0 0 のワンチップ化が可能になる。なお、こうしたワンチップ化の他の例として、例えば特開 2 0 0 0 - 2 4 2 7 7 1 に開示されたものがある。

## 【 0 0 1 6 】

図 1 3 (a) は、容量検出回路 2 1 8 の回路図である。図 1 3 (a) において

、 $C_f$ は図12におけるセンサ電極215と指3の皮膚との間に形成される静電容量である。容量 $C_f$ を形成するセンサ電極215はNchMOSトランジスタ $Q_{3a}$ のドレイン端子に接続されており、このトランジスタ $Q_{3a}$ のソース端子は電流 $I$ の電流源21aの入力側に接続されている。また、センサ電極215とトランジスタ $Q_{3a}$ との節点 $N_{1a}$ には、NchMOSトランジスタ（第1の素子） $Q_{2a}$ のソース端子が接続されている。このトランジスタ $Q_{2a}$ のドレイン端子には、ソース端子に電源電圧 $V_{DD}$ が印加されたPchMOSトランジスタ（第1のスイッチ手段） $Q_{1a}$ のドレイン端子と、ドレイン端子に電源電圧 $V_{DD}$ が印加されソース端子が抵抗 $R_a$ を介して接地に接続されたNchMOSトランジスタ $Q_{4a}$ のゲート端子とが接続されている。このトランジスタ $Q_{4a}$ のソース端子にインバータゲート41が接続されている。

## 【0017】

各トランジスタ $Q_{1a}$ 、 $Q_{3a}$ のゲート端子にはそれぞれ信号 $PRE$ （バー）、 $RE$ が印加される。また、トランジスタ $Q_{2a}$ のゲート端子には定電圧源からバイアス電圧 $V_G$ が印加される。ここで、トランジスタ $Q_{2a}$ が非導通状態になるゲート－ソース間のしきい値電圧を $V_{th}$ とすると、 $V_{DD} > V_G - V_{th}$ となるように電圧 $V_{DD}$ 、 $V_G$ が設定される。

また、節点 $N_{1a}$ 、 $N_{2a}$ はそれぞれ寄生容量 $C_{p1a}$ 、 $C_{p2a}$ を有している。

## 【0018】

図13（b）～図13（d）は、図13（a）に示した容量検出回路218の動作を説明するためのタイミングチャートであり、図13（b）はトランジスタ $Q_{1a}$ を制御する信号 $PRE$ （バー）の電位変化を示し、図13（c）はトランジスタ $Q_{3a}$ を制御する信号 $RE$ の電位変化を示し、図13（d）は節点 $N_{1a}$ 、 $N_{2a}$ それぞれの電位変化を示している。

最初、トランジスタ $Q_{1a}$ のゲート端子には $High$ レベル（ $V_{DD}$ ）の信号 $PRE$ （バー）が与えられ、トランジスタ $Q_{3a}$ のゲート端子には $Low$ レベル（ $GND$ ）の信号 $RE$ が与えられている。したがって、このときトランジスタ $Q_{1a}$ 、 $Q_{3a}$ はともに導通していない。

## 【0019】

この状態で信号PRE（バー）がHighレベルからLowレベルに変化すると、トランジスタQ1aが導通状態になる。このときトランジスタQ3aは非導通状態のままであり、信号発生回路20は停止状態にあるから、節点N2aの電位がVDDにプリチャージされる。

また、トランジスタQ2aのゲートソース間電圧がしきい値電圧 $V_{th}$ に達してトランジスタQ2aが非導通状態になるまで、節点N1aが充電される。これにより、節点N1aの電位が $V_G - V_{th}$ にプリチャージされる。

## 【0020】

プリチャージが終了した後、信号PRE（バー）がHighレベルに変化すると、トランジスタQ1aが非導通状態になる。これと同時に信号REがHighレベルに変化すると、トランジスタQ3aが導通状態になり、信号発生回路20が動作状態に変化する。そして、電流源21aにより節点N1aに充電された電荷が引き抜かれ、節点N1aの電位がわずかに低下すると、トランジスタQ2aのゲートソース間電圧がしきい値電圧 $V_{th}$ より大きくなり、トランジスタQ2aが導通状態に変化する。これにより節点N2aの電荷も引き抜かれ、節点N2aの電位低下が開始する。

信号REをHighレベルにする期間を $\Delta t$ とすると $\Delta t$ 経過後の節点N1aの電位低下 $\Delta V$ は $V_{DD} - (V_G - V_{th}) + I \Delta t / (C_f + C_{p1a})$ になる。ここで、寄生容量 $C_{p2a}$ は寄生容量 $C_{p1a}$ に対して十分小さいとしている。

## 【0021】

電流源21aの電流 $I$ と期間 $\Delta t$ と寄生容量 $C_{p1a}$ 、 $C_{p2a}$ は、各々一定であるから、電位低下 $\Delta V$ は、センサ電極215と検出対象である指の表面3との間に発生する容量の値 $C_f$ によって決定される。この容量値 $C_f$ はセンサ電極215と指の表面3との距離によって決まるので、指紋の凹凸によって異なる。このことから、低下電位 $\Delta V$ の大きさが、指紋の凹凸を反映して変化する。この電位低下 $\Delta V$ が、入力信号として出力回路40に供給されるので、出力回路40で $\Delta V$ が入力され、指紋の凹凸を反映した信号が出力回路40から出力される。

こうした各容量検出回路218の出力信号が処理装置203により処理され、

前述の指紋画像データとして生成される。

#### 【 0 0 2 2 】

次に、上記のような指紋センサ 2 0 2 を有する指紋認証トークン 1 0 6 による利用者本人の認証動作を図 9 のフローチャートを参照して説明する。

利用者が指紋認証トークン 1 0 6 の指紋センサ 2 0 2 上に自身の指をのせる（と（ステップ S 4 1））、指紋認証トークン 1 0 6 の処理装置 2 0 3 は、指紋センサ 2 0 2 により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する（ステップ S 4 2）。ここで、指紋認証トークン 1 0 6 の記憶装置 2 0 4 には、予め指紋センサ 2 0 2 により検出され処理装置 2 0 3 により処理された利用者自身の指紋画像データ中の特徴部分を示す照合情報が登録されており、処理装置 2 0 3 は、記憶装置 2 0 4 に保存されているこの登録情報と、ステップ S 4 2 で抽出した照合情報とを比較する（ステップ S 4 3）。そして、双方の照合情報が一致してステップ S 4 4 の「照合情報が一致？」の判定が Y E S となると、処理装置 2 0 3 は、利用者本人であることを認証する（ステップ S 4 5）。

#### 【 0 0 2 3 】

次に、以上のような指紋認証トークン 1 0 6 を用いた本システムの動作を図 5 ～図 8 のフローチャートを参照して説明する。

##### （第 1 の実施の形態）

まず、図 5 及び図 6 のフローチャートを用いて本システムの第 1 の実施の形態の動作を説明する。

利用者が例えばコンサート会場でのコンサートを聴く場合、予めチケットを購入することになるが、この場合利用者は図 5 のステップ S 1 で例えばチケット販売店や自宅のクレードル 1 0 1 に自身の指紋認証トークン 1 0 6 を挿入し、チケット販売店にチケット代金の支払いを行う（ステップ S 2）。

#### 【 0 0 2 4 】

すると、クレードル 1 0 1 はパスワードを発行し指紋認証トークン 1 0 6 に送信する（ステップ S 3）。指紋認証トークン 1 0 6 の処理装置 2 0 3 はこのパスワードを受信すると記憶装置 2 0 4 に記憶する（ステップ S 4）。また、クレ

ドル106は、発行したパスワードをネットワーク105を介してデータベース102に送信し、データベース102に保存させる（ステップS5）。

【0025】

こうして、チケット代金を支払いパスワードが記録された指紋認証トークン106を所持した利用者は、コンサート開演の当日そのコンサート会場に赴くことになる。なお、この場合、利用者は前述の指紋認証トークン106に図3または図4に示すアダプタを付加した無線通信ユニット107または赤外線通信ユニット108として所持する。

【0026】

図6のフローチャートはこのときのシステムの動作を示すフローチャートである。

コンサート会場の入場ゲート104はステップS11のように閉じたままの状態となっている。ここで、利用者は所持した無線通信ユニット107または赤外線通信ユニット108を用いて自身の指を指紋センサ202に押捺することにより本人認証を行う（ステップS12）。この場合、無線通信ユニット107または赤外線通信ユニット108の処理装置203は、前述した図9のフローチャートのステップ43に示すように、指紋センサ202により検出された指紋と記憶装置204の登録指紋データとを比較照合する。そして、双方の指紋が一致してステップS13の「本人であるか？」の判定がYESとなると、無線通信ユニット107または赤外線通信ユニット108は、チケット購入時に指紋認証トークン106に保存したパスワードを無線信号または赤外線信号に変換して、ゲート104近傍の無線／赤外線信号受信装置109へ送信する（ステップS14）。この無線信号または赤外線信号によるパスワードは無線／赤外線信号受信装置109により受信される。

【0027】

ゲートコントローラ103は、無線／赤外線信号受信装置109を介してこのパスワードを取得すると（ステップS15）、取得したパスワードとデータベース102に保存されているパスワードと比較する（ステップS16）。そして、双方のパスワードが一致しステップS17の判定がYESとなると、ゲート10

4を開放する（ステップS18）。これにより、利用者はコンサート会場へ入場することができる。なお、競技場で試合を観戦する場合も同様である。

#### 【0028】

このように、例えばコンサートのチケット購入時に利用者がその代金を支払うと、データベース102及び利用者の指紋認証トークン106にパスワードを記憶するとともに、コンサート会場の入場時に利用者が所持した指紋認証トークン106により利用者本人の確認を行い、利用者本人であることが認証されて指紋認証トークン106から入場ゲート104近傍の無線／赤外線信号受信装置109へパスワードが送信されると、このパスワードを無線／赤外線信号受信装置109を介して受信したゲートコントローラ103は、データベース102のパスワードとの比較を行い双方のパスワードが一致すると入場ゲート104を開放するようにしたものである。この結果、コンサート会場や競技場への入場時にはチケットが不要になり、したがって、チケットのチェック要員を無くすことができるとともに、利用者はコンサート会場や競技場へ速やかに入場できる。また、利用者の指紋認証トークン106が盗難され、その指紋認証トークン106を利用して第三者が不正に入場しようとしても、利用者の指紋画像と異なることから第三者による不正入場を阻止できる。また、指紋認証トークン106を紛失した場合、新たな指紋認証トークンを用い図5の各ステップに示す手順と同様の手順を行うことによりチケットの再発行を行うことができる。

#### 【0029】

（第2の実施の形態）

次に、図7及び図8を参照して、本システムの第2の実施の形態の動作を説明する。

利用者がコンサート会場でコンサートを聴く場合、予め利用者は図7のステップS21でチケット販売店や自宅のクレードル101に自身の指紋認証トークン106を挿入し、チケット販売店にチケット代金の支払いを行う（ステップS22）。

#### 【0030】

すると、指紋認証トークン106は、予め記憶装置204に付与されている識

別番号をクレードル101に送信する（ステップS23）。クレードル101はこの識別番号を受信すると、受信した識別番号をネットワーク105を介してデータベース102に送信し、データベース102に保存させる（ステップS24）。

#### 【0031】

こうして、チケット代金を支払うことにより、自身の識別番号をデータベース102に保存した指紋認証トークン106を所持した利用者は、コンサート開演の当日そのコンサート会場に赴くことになる。なお、この場合、利用者は前述の指紋認証トークン106に図3または図4に示すアダプタを付加した無線通信ユニット107または赤外線通信ユニット108として所持する。

#### 【0032】

図8のフローチャートはこのときのシステムの動作を示すフローチャートである。

コンサート会場の入場ゲート104はステップS31のように閉じたままの状態となっている。ここで、利用者は所持した無線通信ユニット107または赤外線通信ユニット108を用いて自身の指を指紋センサ202に押捺することにより本人認証を行う（ステップS32）。この場合、無線通信ユニット107または赤外線通信ユニット108の処理装置203は、前述した図9のフローチャートのステップ43に示すように、指紋センサ202により検出された指紋と記憶装置204の登録指紋データとを比較照合する。そして、双方の指紋が一致してステップS33の「本人であるか？」の判定がYESとなると、無線通信ユニット107または赤外線通信ユニット108は、予め指紋認証トークン106に付与されている識別番号を無線信号または赤外線信号に変換して、ゲート104近傍の無線／赤外線信号受信装置109へ送信する（ステップS34）。この無線信号または赤外線信号による識別番号は無線／赤外線信号受信装置109により受信される。

#### 【0033】

ゲートコントローラ103は、無線／赤外線信号受信装置109を介してこの識別番号を取得すると（ステップS35）、取得した識別番号とデータベース1

02に保存されている識別番号と比較する（ステップS36）。そして、双方の識別番号が一致しステップS37の判定がYESとなると、ゲート104を開放する（ステップS38）。これにより、利用者はコンサート会場へ入場することができる。なお、競技場で試合を観戦する場合も同様である。

#### 【0034】

このように、例えばコンサートのチケット購入時に利用者がその代金を支払うと、利用者の指紋認証トークン106に付与されている識別番号をデータベース102に記憶するとともに、コンサート会場の入場時に利用者が所持した指紋認証トークン106により利用者本人の確認を行い、利用者本人であることが認証されて指紋認証トークン106から入場ゲート104近傍の無線／赤外線信号受信装置109へ識別番号が送信されると、この識別番号を無線／赤外線信号受信装置109を介して受信したゲートコントローラ103は、データベース102の識別番号との比較を行い双方の識別番号が一致すると入場ゲート104を開放するようにしたものである。この結果、コンサート会場や競技場への入場時にはチケットが不要になり、したがって、チケットのチェック要員を無くすことができるとともに、コンサート会場や競技場へ速やかに入場できる。また、利用者の指紋認証トークン106が盗難され、その指紋認証トークン106を利用して第三者が不正に入場しようとしても、利用者の指紋画像と異なることから第三者による不正入場を阻止できる。また、指紋認証トークン106を紛失した場合、新たな指紋認証トークンを用い図7の各ステップに示す手順を再度行うことによりチケットの再発行を行うことができる。

#### 【0035】

なお、本実施の形態では、パスワードまたは識別番号を用いてゲート104を開放するようにしたが、ワンタイムパスワードを用いるようにしても良い。

また、本実施の形態では、利用者の入場ゲート4の通過時に無線通信ユニット107または赤外線通信ユニット108から無線信号または赤外線信号によるパスワードや識別番号等を送信するようにしたが、ゲート104の近傍にゲートコントローラ103に接続され指紋認証トークン106が挿入可能なクレードルを設ければ、指紋認証トークン106のみによりゲート104を通過できる。



また、本実施の形態では、利用者のチケット購入時にチケット販売店や自宅のクレードル101に指紋認証トークン106を挿入するようにしているが、チケット販売店や自宅のクレードル101に無線／赤外線信号受信装置を設ければ、無線通信ユニット107または赤外線通信ユニット108によりチケットを購入することができる。

## 【0036】

また、本実施の形態では、無線通信ユニットとして図3に示すような構造の無線通信ユニット107を用いるようにしたが、図10に示すような腕時計型の構造を有するものや、ブレスレット型、或いはペンダント型の構造を有するものであっても良い。なお、赤外線通信ユニット108の構造についても前述した無線通信ユニットの構造と同様の構造を有するものであっても良い。

## 【0037】

また、本実施の形態では、図1に示すようにデータベース102とゲートコントローラ103が専用線で結ばれた例を説明したが、図11に示すようにデータベース102とゲートコントローラ103をネットワーク105を介して接続するようにしても良い。

ここで、データベース102は、図1及び図12には示されていないが、サーバ機能を含むものである。このサーバ機能は、ネットワーク105に接続されたものであれば、データベース102と一体でなくても良く、クレードル101やゲートコントローラ103が代替しても良い。さらに、1つのサーバでシステム全体の制御を行わずに、クレードル101とゲートコントローラ103とで分散して処理するようにしても良い。

## 【0038】

また、本実施の形態では、指紋認証トークン106内の指紋センサ202、処理装置203、記憶装置204をワンチップで構成した第1の構成例について説明したが、上記第1の構成例の他に、指紋センサ202をワンチップ化し、このワンチップ指紋センサ202に、バスを介して処理装置203を接続し、さらに処理装置203にバスを介して記憶装置204を接続する第2の構成例がある。さらに、指紋センサ202と処理装置203をワンチップ化し、このワンチップ

化された処理装置203にバスを介して記憶装置204を接続する第3の構成例がある。

#### 【0039】

また、指紋認証トークン106とクレードル101間、クレードル101とデータベース102間、データベース102とゲートコントローラ103間、及び無線通信ユニット107または赤外線通信ユニット108と無線／赤外線信号受信装置109間で、それぞれ送受される信号を送信側で暗号化し、受信側でその暗号化データを復号化することにより、システムのセキュリティを向上させることができる。

また、本実施の形態では、指紋の認証に基づいてゲート104の開閉を制御するようにしたが、指の大きさ、手形、静脈パターン、人相、虹彩及び声紋などの利用者固有の生体情報や、利用者のサイン（筆跡）等により利用者本人であることを認証してゲート104を開放するようにしても良い。

#### 【0040】

図14は、前述の指紋認証トークン106を含む利用者固有の生体情報や利用者のサイン等により認証を行う認証トークン300と、認証トークン300の認証を利用してゲート104の開閉を制御する前述のゲートコントローラ103を含む利用機器400とからなる認証システムの構成を示すブロック図である。

この認証システムでは、ユーザ固有の生体情報として指紋を用いる場合を例として説明する。

#### 【0041】

認証トークン300には、指紋（生体情報）を読み取るセンサ311（図2の指紋センサ202に対応）、ユーザ本人の登録指紋データ312Aやユーザ情報312Bを記憶する記憶回路312（図2の記憶装置204に対応）、センサ311での読み取り結果を示すセンシングデータ311Aを、記憶回路312に記憶されている登録指紋データ312Aを用いて照合する照合回路313（図2の処理装置203に対応）、この照合回路313での照合結果を含む認証データ313Aを通信データ301Aとして認証トークン300の外部へ送信する通信回路314（図2の処理装置203に対応）が設けられており、これら回路部を一

体として形成する認証トークン 3 0 0 が利用機器 4 0 0 に対して着脱自在に接続される。

利用機器 4 0 0 には、認証トークン 3 0 0 からの通信データ 3 0 1 A を受信する通信回路 4 2 1 と、受信した通信データ 3 0 1 A に含まれる照合結果が一致を示す場合にのみ、そのユーザへのサービス提供を行う処理装置 4 2 2 とが設けられている。

#### 【 0 0 4 2 】

次に、図 1 4 に示す認証システムの動作について説明する。

ユーザは事前に、自分の所持する認証トークン 3 0 0 の記憶回路 3 1 2 に、自分の登録指紋データ 3 1 2 A やサービスを利用するためのパスワードや個人情報などからなるユーザ情報 3 1 2 B を記憶させておく。

利用機器 4 0 0 を利用する際、まずユーザは自分の認証トークン 3 0 0 を利用機器 4 0 0 へ接続し、指をそのセンサ 3 1 1 へ置く。これにより認証トークン 3 0 0 のセンサ 3 1 1 でユーザの指紋が読み取られセンシングデータ 3 1 1 A として出力される。このセンシングデータ 3 1 1 A は照合回路 3 1 3 において記憶回路 3 1 2 の登録指紋データ 3 1 2 A を用いて照合される。そして、その照合結果を含む認証データ 3 1 3 A が出力される。このとき照合回路 3 1 3 は、予め記憶回路 3 1 2 に格納されているユーザ ID、パスワード、個人情報などのユーザ情報 3 1 2 B を読み出し、認証データ 3 1 3 A へ含めて出力する。なお、認証トークン 3 0 0 から出力する情報は、これらの情報の中から選択することができ、本発明のゲート開閉システムでは、パスワードまたは識別情報のみでも良いし、必要に応じてその他の情報を付加しても良い。

#### 【 0 0 4 3 】

通信回路 3 1 4 では、照合回路 3 1 3 からの認証データ 3 1 3 A を通信データ 3 0 1 A として利用機器 4 0 0 へ送信する。

利用機器 4 0 0 の通信回路 4 2 1 では、認証トークン 3 0 0 の通信回路 3 1 4 から送信された通信データ 3 0 1 A を受信し、認証データ 3 1 3 A と同じ内容の認証データ 4 2 1 A として出力する。処理装置 4 2 2 では、この認証データ 4 2 1 A を受け取ってその認証データ 4 2 1 A に含まれる照合結果を参照する。そし

て、その照合結果が一致を示す場合、処理装置 4 2 2 においてユーザの所望する所定の処理が実行される。

## 【 0 0 4 4 】

このように、ユーザの指紋を検出しその検出結果をセンシングデータとして出力するセンサ 3 1 1 と、ユーザの指紋を照合するための登録指紋データ 3 1 2 A が予め格納されている記憶回路 3 1 2 と、この記憶回路 3 1 2 に記憶されている登録指紋データ 3 1 2 A を用いてセンサ 3 1 1 からのセンシングデータ 3 1 1 A を照合し、ユーザ認証結果となるその照合結果を認証データとして出力する照合回路 3 1 3 と、この照合回路 3 1 3 からの認証データを通信データ 3 0 1 A として利用機器 4 0 0 へ送信する通信回路 3 1 4 とを、認証トークン 3 0 0 として一体として形成したものである。

## 【 0 0 4 5 】

そして、認証に応じて所定の処理を行う利用機器 4 0 0 をユーザが利用する場合には、認証トークン 3 0 0 をその利用機器 4 0 0 へ接続し、その認証トークン 3 0 0 でユーザの生体情報に基づきユーザ認証を行い、利用機器 4 0 0 へ通知するようにしたものである。

また、利用機器 4 0 0 に、認証トークン 3 0 0 から送信された通信データ 3 0 1 A を受信し認証データ 4 2 1 A として出力する通信回路 4 2 1 と、この通信回路 4 2 1 からの認証データ 4 2 1 A に含まれる照合結果に基づき所定の処理を行う処理装置 4 2 2 とを設け、この利用機器 4 0 0 とは独立した各ユーザが個々の持つ認証トークン 3 0 0 での認証結果に基づき所定の処理を行うようにしたものである。

## 【 0 0 4 6 】

したがって、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることがなくなり照合時に用いる登録データの漏洩を防止できる。また、センサを不特定多数のユーザで共用する必要がなく、ユーザが個々に所持する認証トークンごとに設けられているセンサを用いるため、センサ故障が発生しても他のユーザには波及

せず、さらに生体情報検出の際、指紋などのようにセンサに対して人体の一部を接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。なお、認証トークン300については、センサ、記憶回路および照合回路などを1チップの半導体装置として形成する技術（例えば、特開2000-242771号公報など参照）を用いることで、非常に小型な認証トークンを実現することも可能となる。

## 【0047】

さらに、記憶回路312にユーザIDやパスワードさらには個人情報などのユーザ情報312Bを予め記憶しておき、これらを認証データ313Aに含めて利用機器400へ送信するようにしたので、利用機器400の処理装置422において、その認証データに含まれるユーザ情報312B、例えばユーザIDやパスワードをチェックすることにより処理実行の可否を判断でき、利用機器で行う処理の重要性に合わせた基準で認証判定できる。また、ユーザ情報312Bの個人情報、例えば氏名、住所、電話番号、口座番号やクレジットカード番号などを処理に用いることにより、処理に必要な個人情報をユーザが入力する必要がなくなり、ユーザの操作負担を大幅に軽減できる。

## 【0048】

なお、利用機器400に図示しない乱数発生回路及び復号回路を設け、かつ認証トークン300に図示しない暗号化回路を設けて、利用機器400と認証トークン300間で通信されるデータの暗号化することにより、セキュリティの向上を図ることができる。

## 【0049】

即ち、利用機器400は、認証トークン300側からのアクセス時に乱数発生回路により乱数を発生させてこの乱数を通信回路421から認証トークン300へ送信して暗号化回路に記憶させる一方、認証トークン300の暗号化回路は照合回路313から出力された認証データ313Aと、記憶した乱数との和を演算してその演算結果を、予め記憶回路312に記憶してある共通鍵により暗号化して暗号化データとして利用機器400側へ送信する。利用機器400では、通信回路421により受信したこの暗号化データを復号回路が共通鍵を用いて復号化

するとともに復号化したデータから乱数発生回路が発生した前記乱数を減算することにより認証データ421Aとして処理回路422へ出力する。なお、上記の例では、認証トークン300及び利用機器400の双方に共通鍵を持たせて、それぞれ暗号化及び復号化を行わせているが、認証トークン300に秘密鍵を、利用機器400に公開鍵を持たせてそれぞれ暗号化処理及び復号化処理を行わせることもできる。

#### 【0050】

次に、図15を参照して、本認証システムの第2の構成例について説明する。図15は、図14に示す第1の構成例のうち、認証トークン300の出力段にデータ変換モジュール330を付加したものである。

このデータ変換モジュール330には、認証トークン300の通信回路314から出力された通信データを、利用機器400で受信・解読可能なデータ形式へ変換するプロトコル変換回路331が設けられている。

#### 【0051】

このように、認証トークン300に着脱自在に取り付けられるデータ変換モジュール330を介して、所望の利用機器400と認証トークン300とを接続するようにしたので、データ形式が異なる利用機器に対しても同一認証トークンを用いたユーザ認証が可能となる。また、様々な形式に対応したデータ変換モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが1つの認証トークンを用いて様々な利用機器を利用することができ、複数の認証トークンを所持する必要がない。

以上では、データ変換モジュール330を認証トークン300に対して着脱自在に取り付ける場合を例として説明したが、認証トークン300内部にプロトコル変換回路331を設けてもよく、さらにコンパクトに構成できる。

#### 【0052】

次に、図16を参照して、本認証システムの第3の構成例について説明する。図16は、図14に示す第1の構成例のうち、認証トークン300の出力段に無線モジュール340を付加したもので、この無線モジュール340は前述の無線通信ユニット107に相当するものである。

この無線モジュール340には、認証トークン300の通信回路314から出力された通信データを、利用機器400で受信・解読可能なデータ形式へ変換するプロトコル変換装置341と、このプロトコル変換装置341からの通信データを無線区間を介して利用機器400へ送信する無線回路342とが設けられている。この場合、利用機器400側にも無線回路423を設ける必要がある。

## 【0053】

このように、認証トークン300に着脱自在に取り付けられる無線モジュール340を用いて、所望の利用機器400と認証トークン300とを接続するようにしたので、ユーザは、認証トークン300を利用機器400に直接接続することなく、例えば自分の手元で認証トークン300を用いてユーザ認証を行いサービスを受けることが可能となる。したがって、利用機器400に対して認証トークン300を接続する作業や、利用機器400に接続されている状態の認証トークン300を用いて認証を行う作業など、認証時のユーザに対する作業負担を大幅に軽減できる。

## 【0054】

なお、利用機器400と認証トークン300の通信プロトコルが同一の場合は、無線モジュール340のプロトコル変換回路341を省略することも可能である。また、無線回路342の代わりに、前述の赤外線通信ユニット108のような赤外線通信回路や超音波通信回路など、無線区間を介してデータ通信可能な通信回路を用いてもよい。

以上では、無線モジュール340を認証トークン300に対して着脱自在に取り付ける場合を例として説明したが、認証トークン300内部に無線回路342やプロトコル変換回路341を設けてもよく、さらにコンパクトに構成できる。

## 【0055】

## 【発明の効果】

以上説明したように本発明によれば、会場の入場ゲートを開閉するゲート開閉システムにおいて、利用者の生体情報に基づき利用者本人を認証する認証トークンと、利用者が前記会場の入場料の前払いを行うと利用者の識別情報が記憶されるデータベースとを設け、利用者の前記会場への入場時に認証トークンにより利

用者が本人であると認証されこの認証トークンに予め記憶されている利用者の識別情報が認証トークンから出力されると、この識別情報を受信するとともに受信した識別情報がデータベース内に記憶されている場合は入場ゲートを開放するようにしたので、利用者がコンサート会場や競技場への入場時にはチケットが不要になり、したがって、チケットのチェック要員を無くすことができるとともに、利用者はコンサート会場や競技場へ速やかに入場できる。また、利用者の認証トークンが盗難され、その認証トークンを利用して第三者が不正に入場しようとしても、利用者の生体情報と異なることから第三者による不正入場を阻止でき、したがって利用者の的確な入場管理を行うことができる。

【図面の簡単な説明】

【図 1】 本発明に係るゲート開閉システムの構成を示すブロック図である。

【図 2】 ゲート開閉システムに用いられる指紋認証トークンの外観を示す図（図 2（a））及びその構成を示すブロック図（図 2（b））である。

【図 3】 ゲート開閉システムに用いられる無線通信ユニットの外観を示す図（図 3（a））及びその構成を示すブロック図（図 3（b））である。

【図 4】 ゲート開閉システムに用いられる赤外線通信ユニットの外観を示す図（図 4（a））及びその構成を示すブロック図（図 4（b））である。

【図 5】 ゲート開閉システムの第 1 の実施の形態の動作を示すフローチャートである。

【図 6】 ゲート開閉システムの第 1 の実施の形態の動作を示すフローチャートである。

【図 7】 ゲート開閉システムの第 2 の実施の形態の動作を示すフローチャートである。

【図 8】 ゲート開閉システムの第 2 の実施の形態の動作を示すフローチャートである。

【図 9】 指紋認証トークンにおける利用者認証動作を示すフローチャートである。

【図 10】 ゲート開閉システムに用いられる他の通信ユニットの例を示す



図である。

【図 1 1】 ゲート開閉システムの他の構成を示すブロック図である。

【図 1 2】 前記指紋認証トークンを構成する指紋センサの詳細構成を示す図である。

【図 1 3】 前記指紋センサ内の容量検出回路の回路図及び前記容量検出回路の各部の動作タイミングを示すタイムチャートである。

【図 1 4】 認証トークンおよび利用機器からなる認証システムの第 1 の構成例を示すブロック図である。

【図 1 5】 認証トークンおよび利用機器からなる認証システムの第 2 の構成例を示すブロック図である。

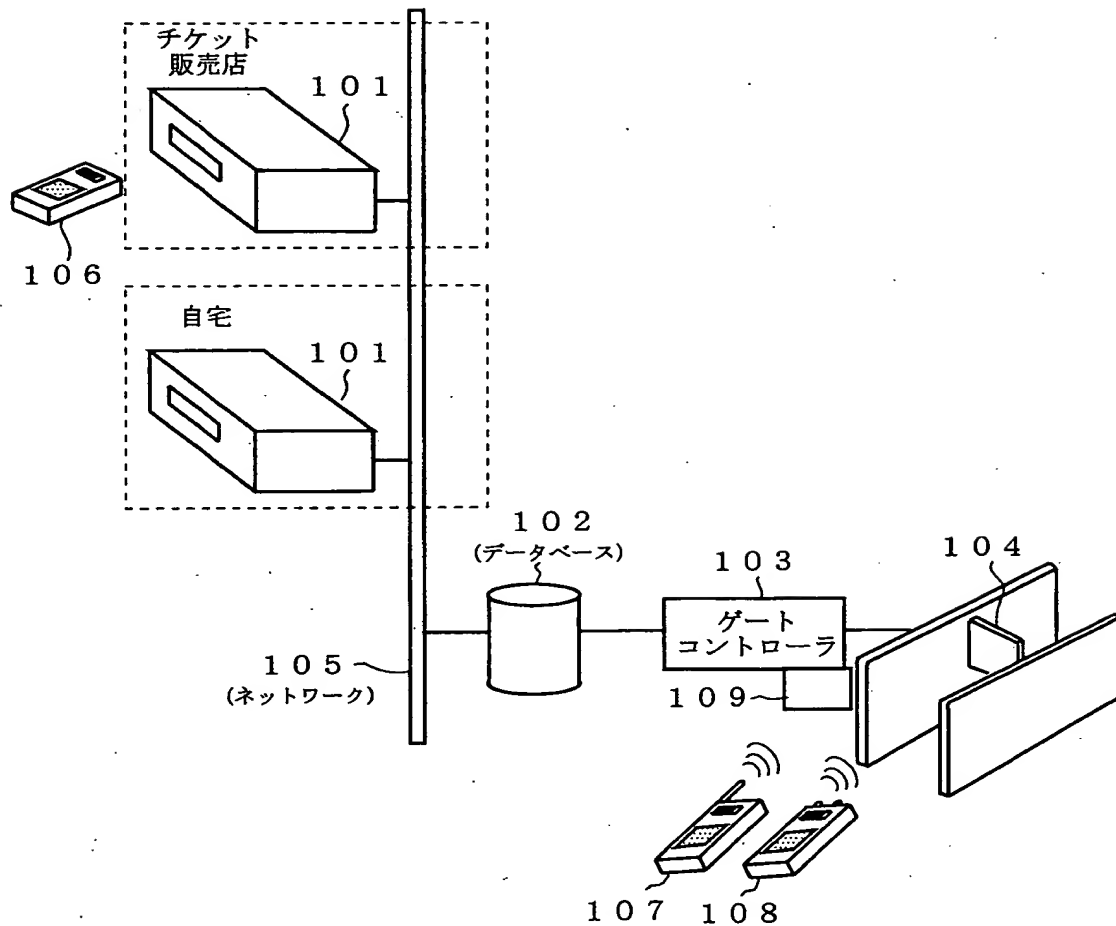
【図 1 6】 認証トークンおよび利用機器からなる認証システムの第 3 の構成例を示すブロック図である。

【符号の説明】

1 0 1 …クレードル、1 0 2 …データベース、1 0 3 …ゲートコントローラ、1 0 4 …ゲート、1 0 5 …ネットワーク、1 0 6 …指紋認証トークン、1 0 7 …無線通信ユニット、1 0 8 …赤外線通信ユニット、1 0 9 …無線／赤外線信号受信装置、2 0 2 …指紋センサ、2 0 3 …処理装置、2 0 4 …記憶装置、2 1 1 …半導体基板、2 1 2 …下層絶縁膜、2 1 3 …配線、2 1 4 …層間絶縁膜、2 1 5 …センサ電極、2 1 7 …パシベーション膜、2 1 8 …容量検出回路、3 0 2 …アンテナ、3 0 3 …無線信号発生回路、4 0 2 …赤外線光源、4 0 3 …赤外線信号発生回路。

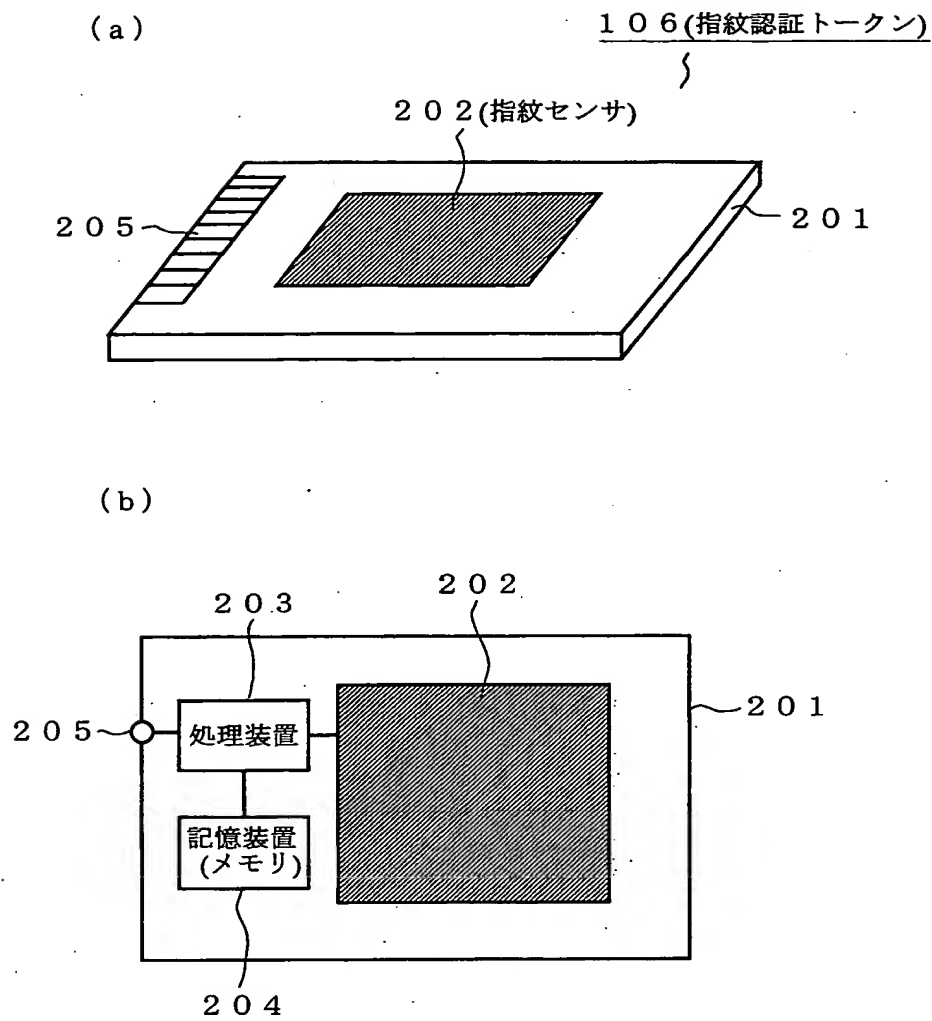
【書類名】 図面

【図 1】

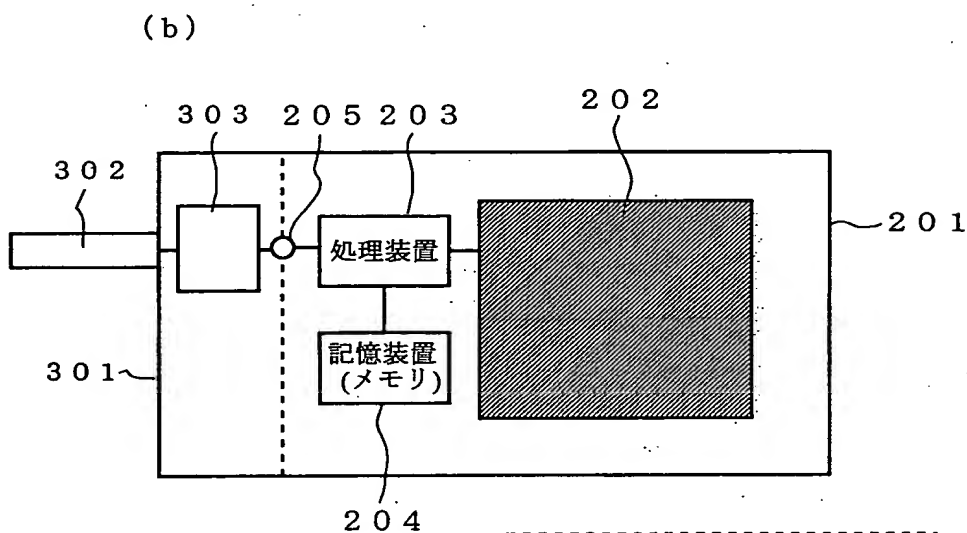
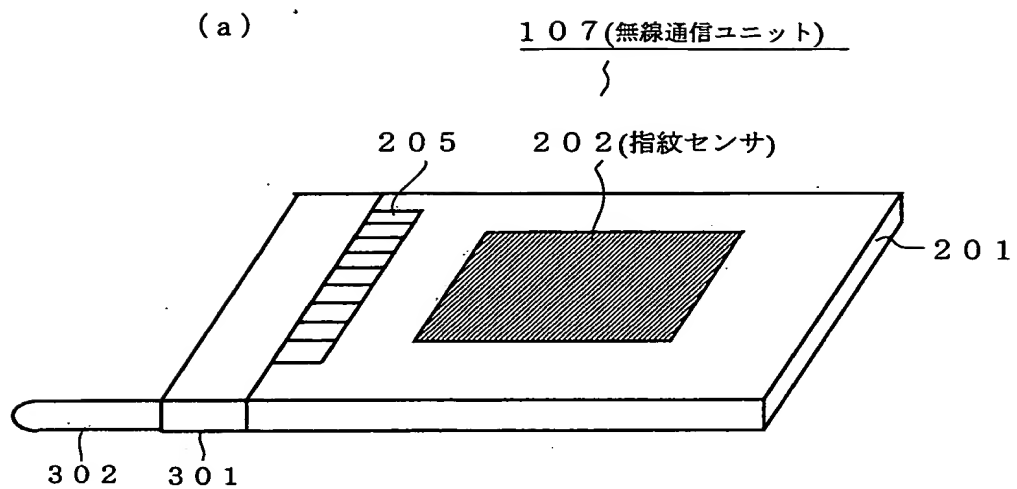


(注) 109 : 無線/赤外線信号受信装置

【図 2】

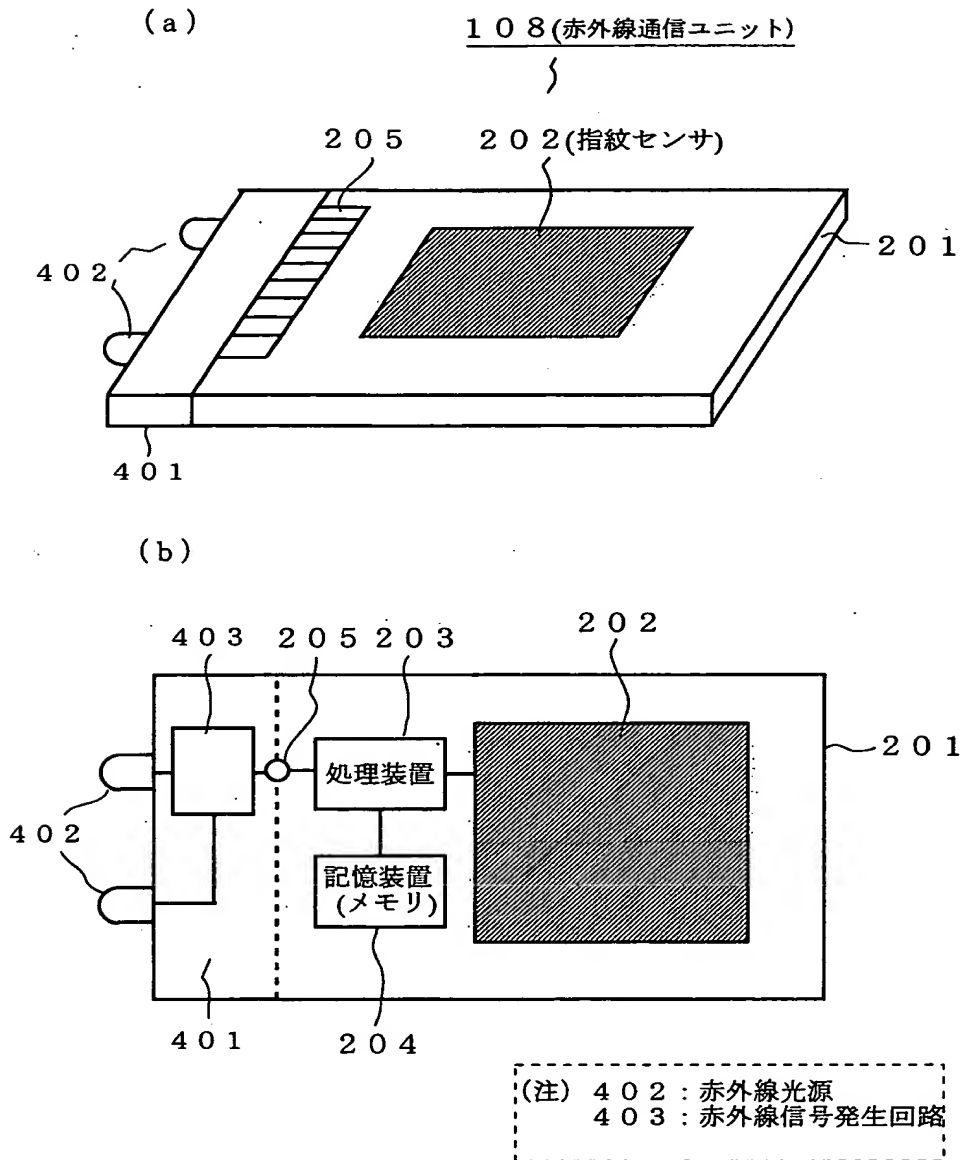


【図 3】

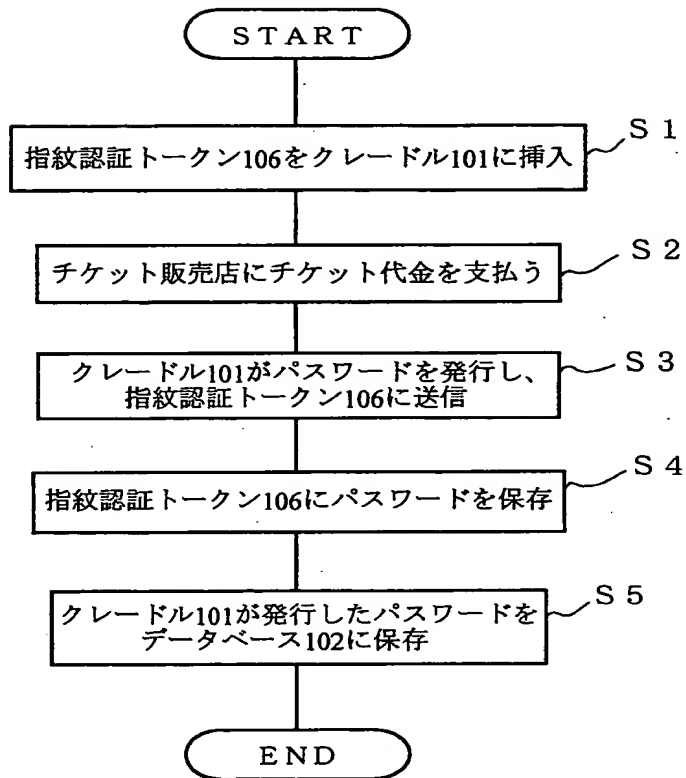


(注) 302 : アンテナ  
303 : 無線信号発生回路

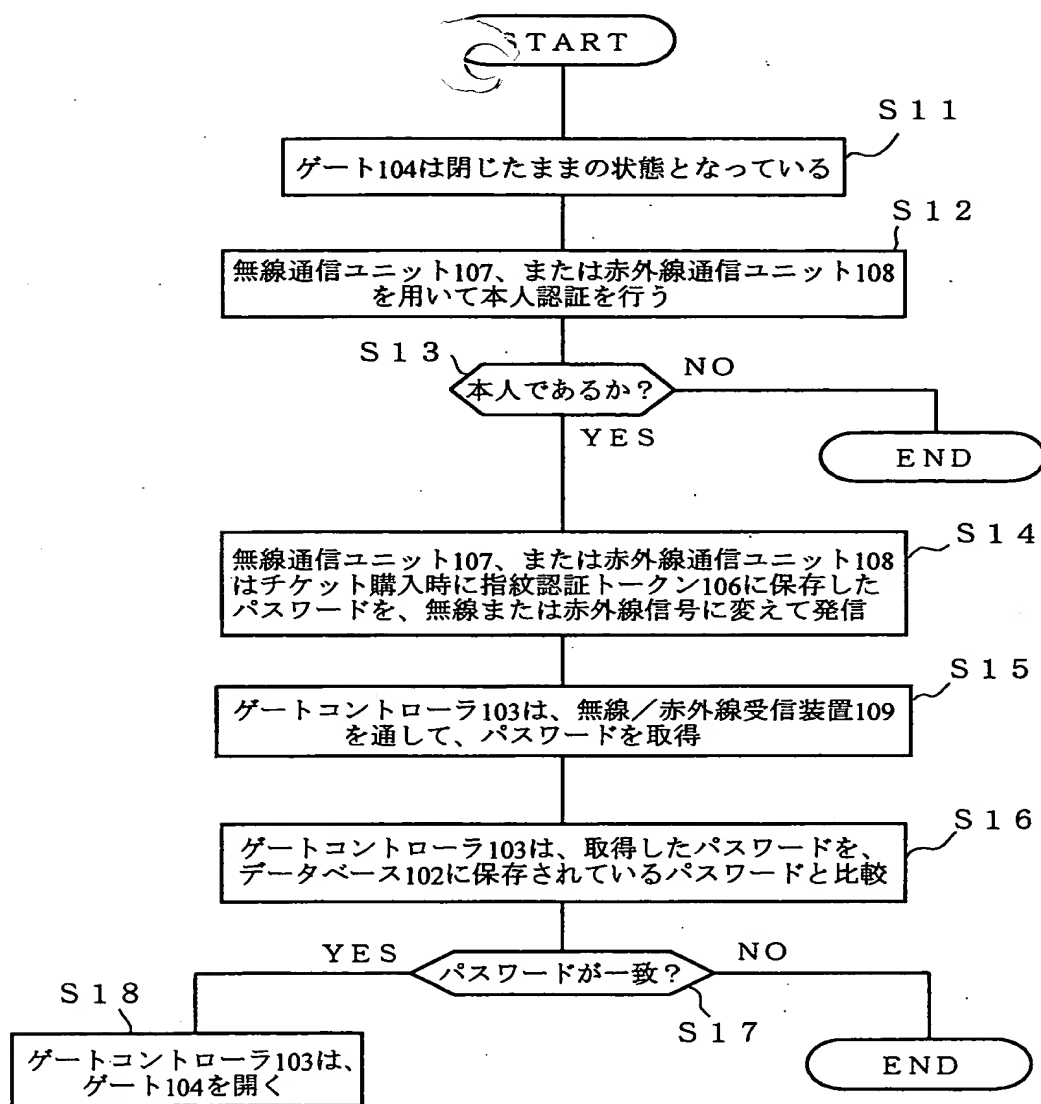
【図4】



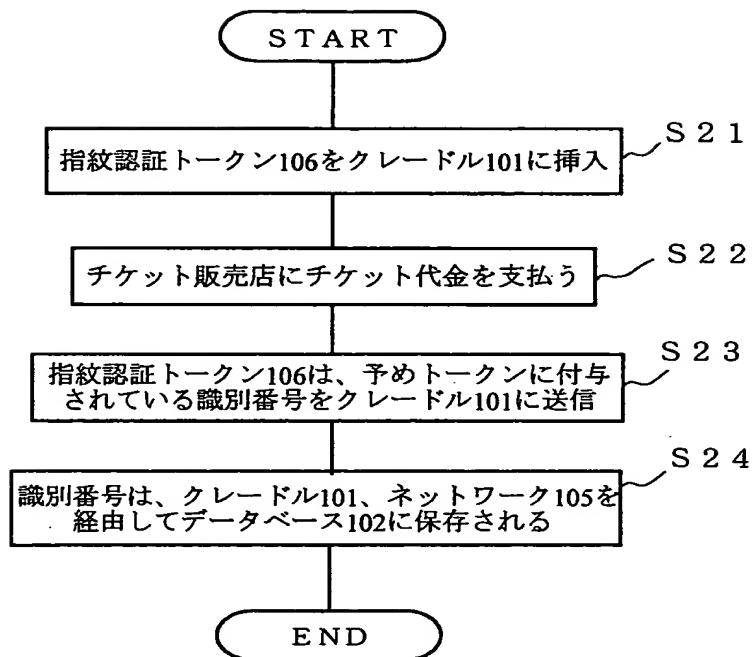
【図 5】



【図 6】

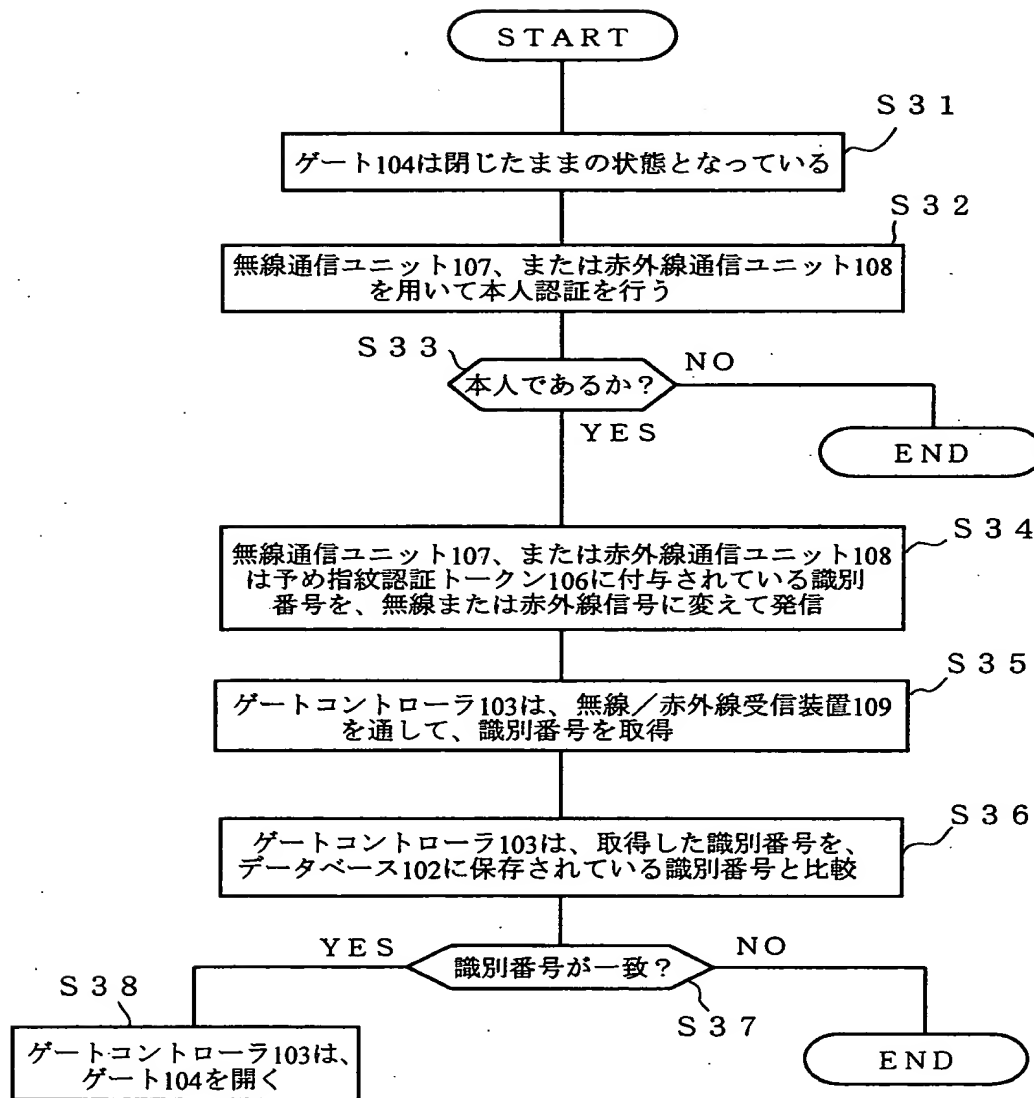


【図 7】

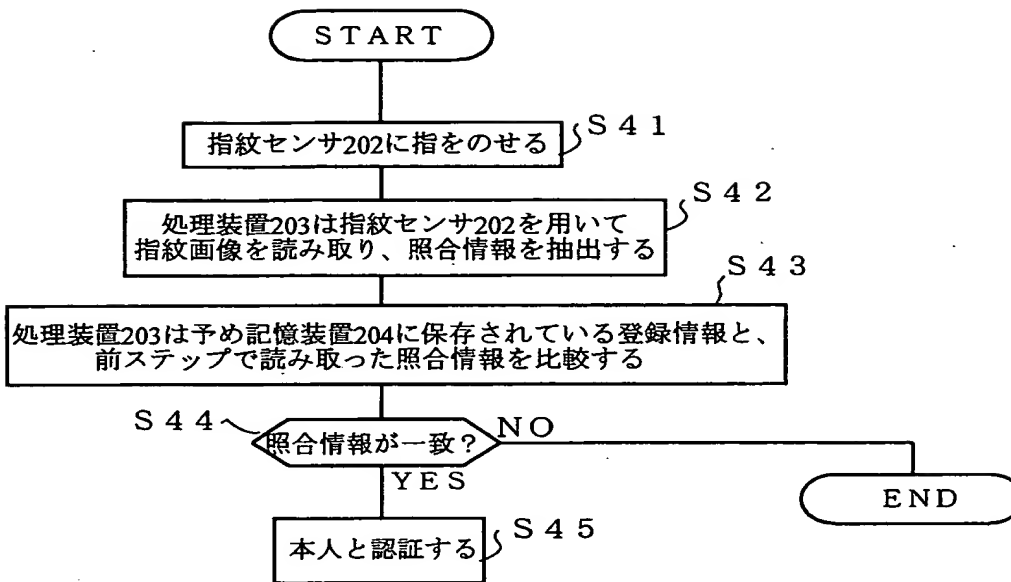




【図 8】

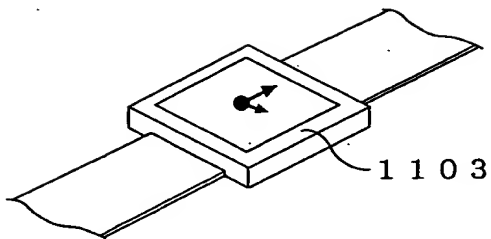


【図 9】

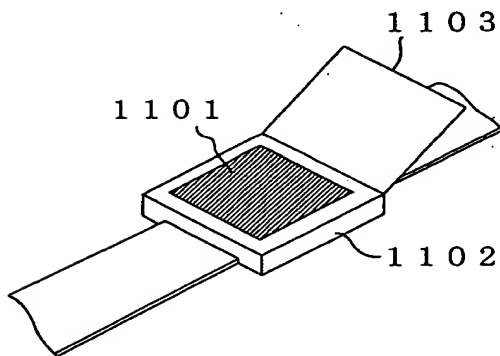


【図10】

(a) 通常時

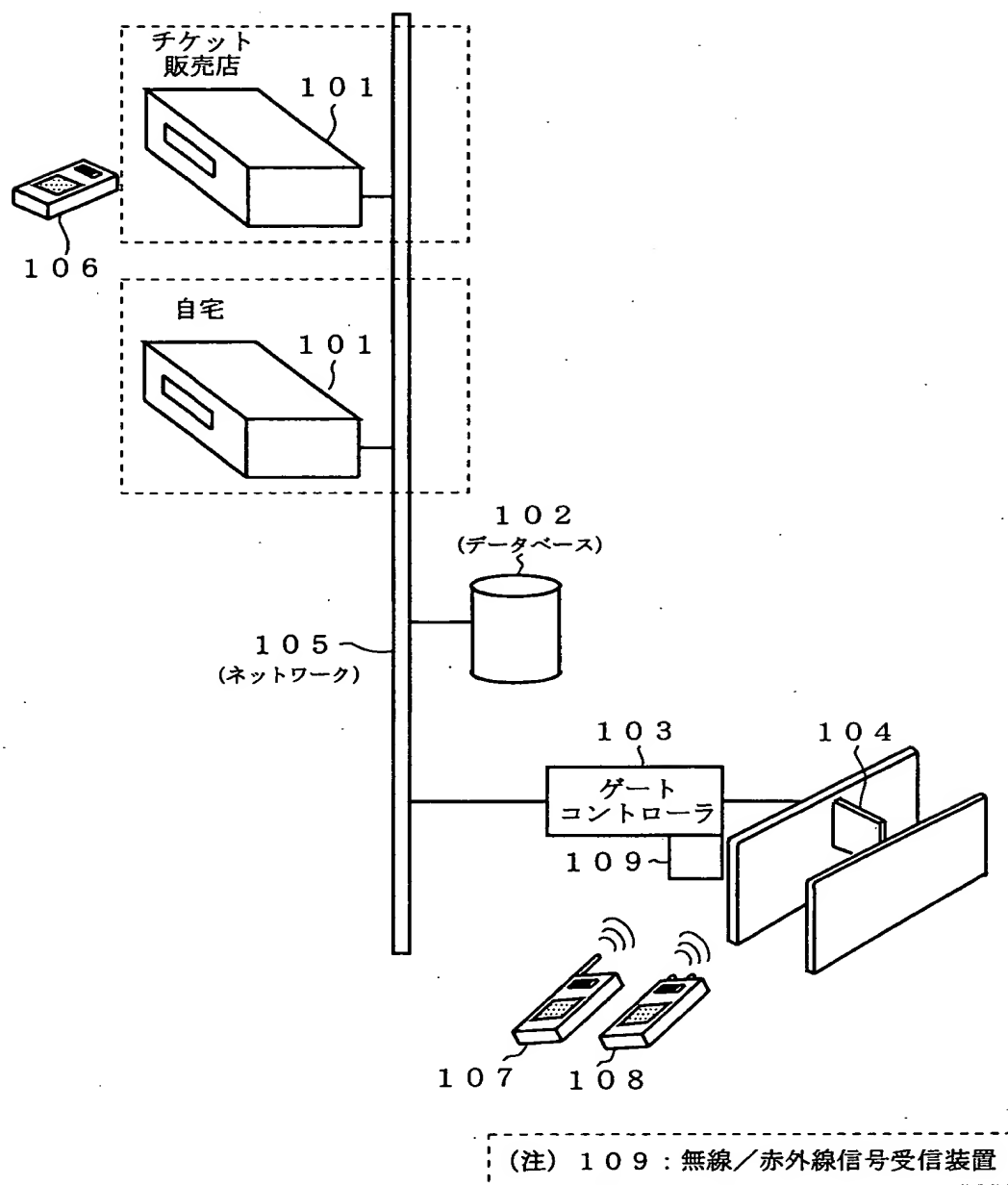


(b) 指紋認証時

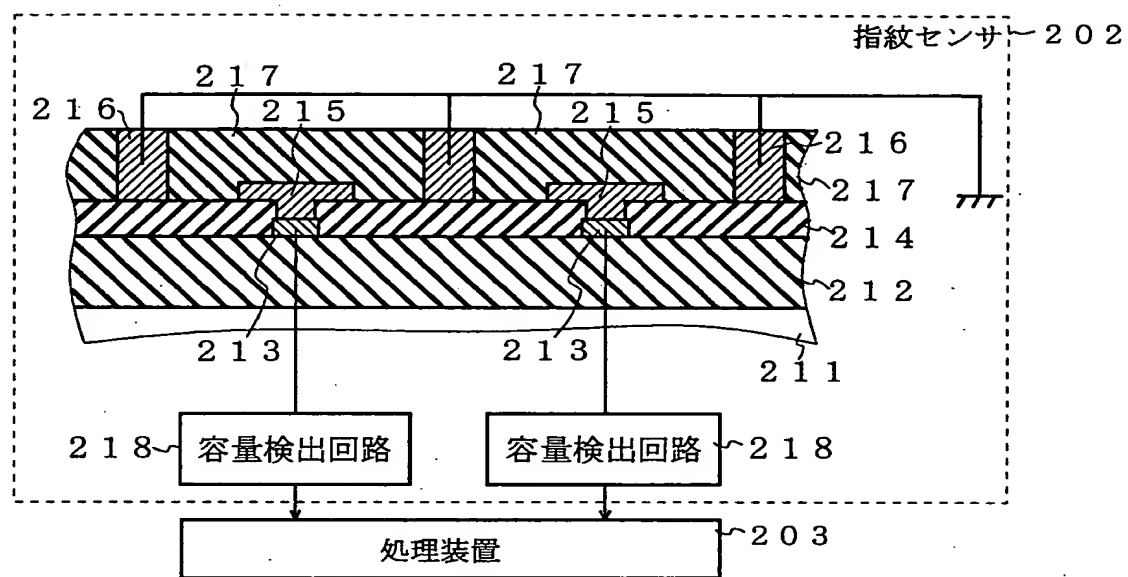


(注) 1101 : 指紋センサ  
1102 : アンテナ  
1103 : 時刻表示部

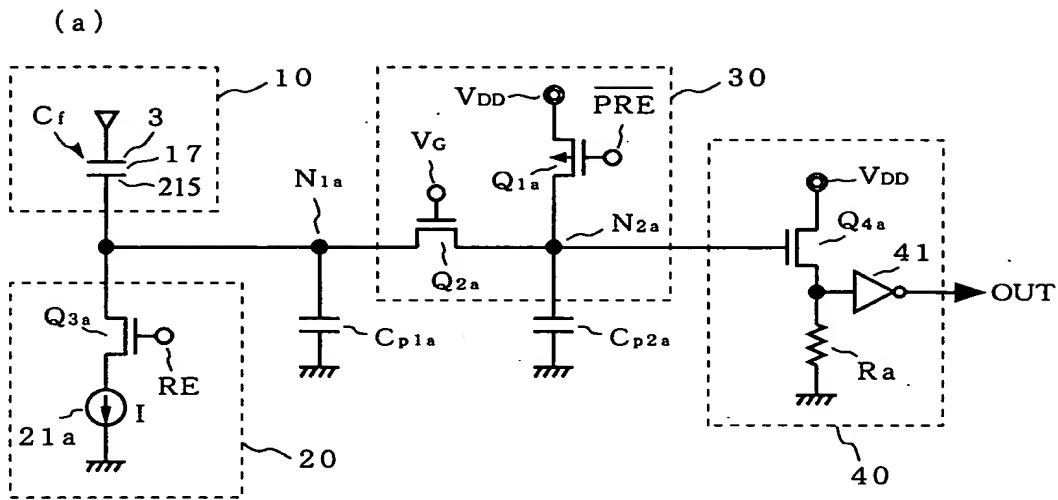
【図 11】



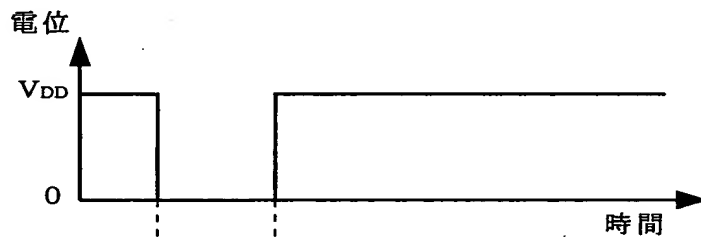
【図 12】



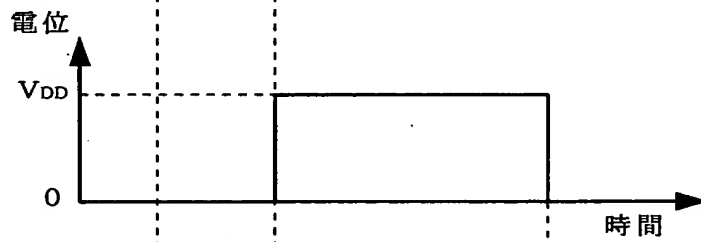
【図 13】



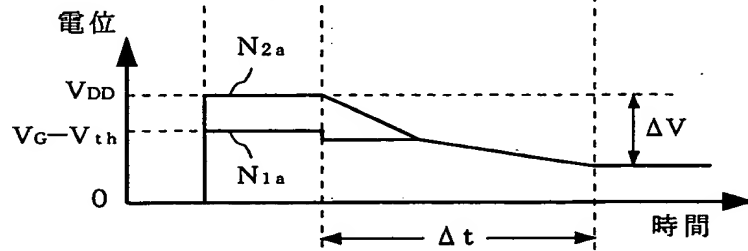
(b)  $\overline{\text{PRE}}$



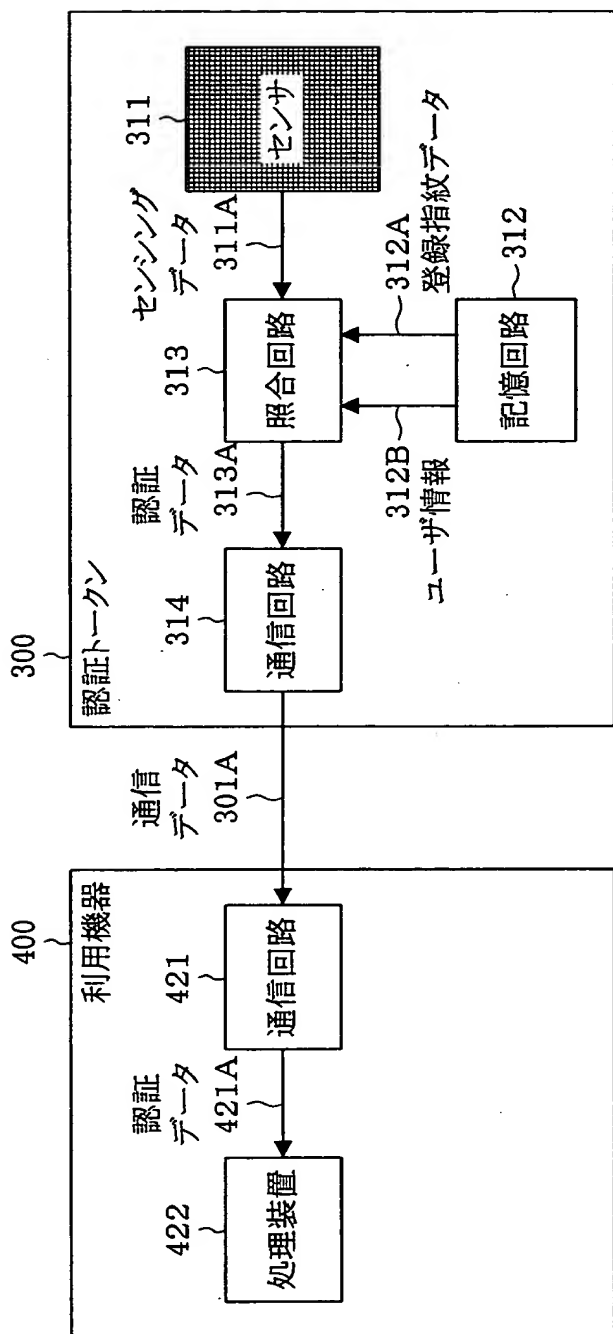
(c) RE



(d)  $N_{1a}, N_{2a}$



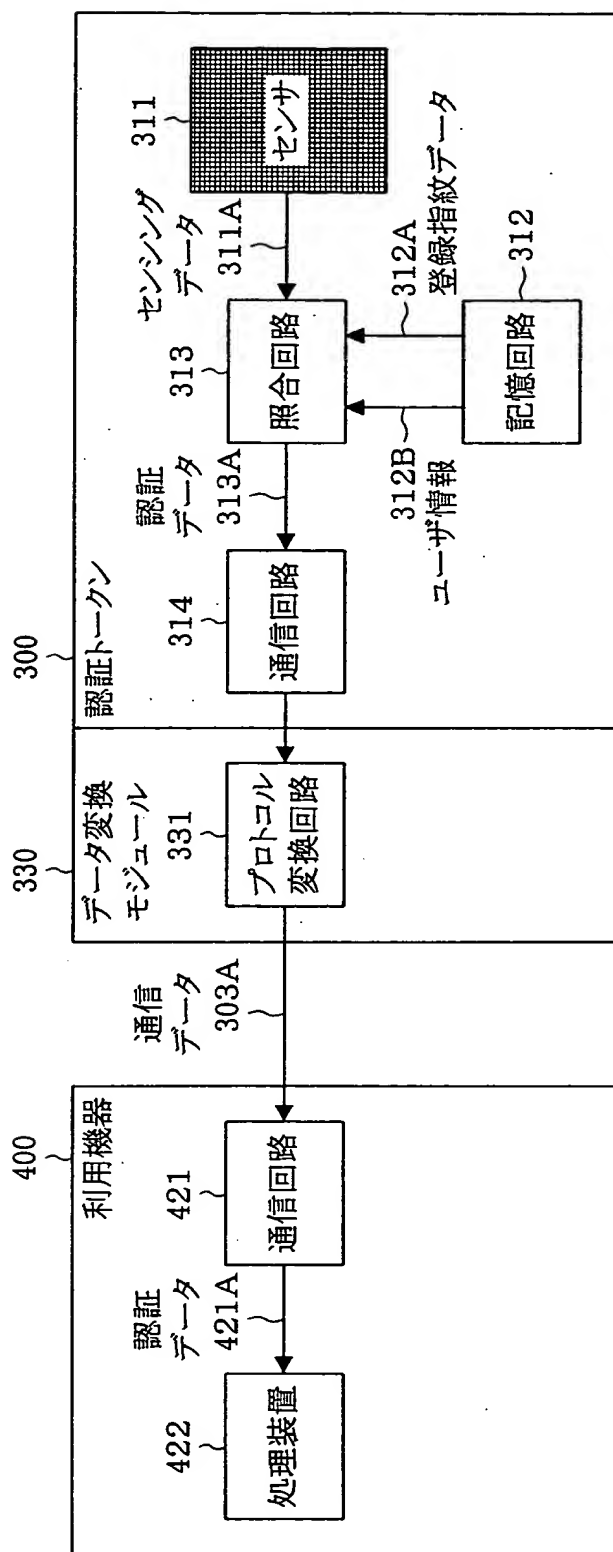
【図 14】



通信データ

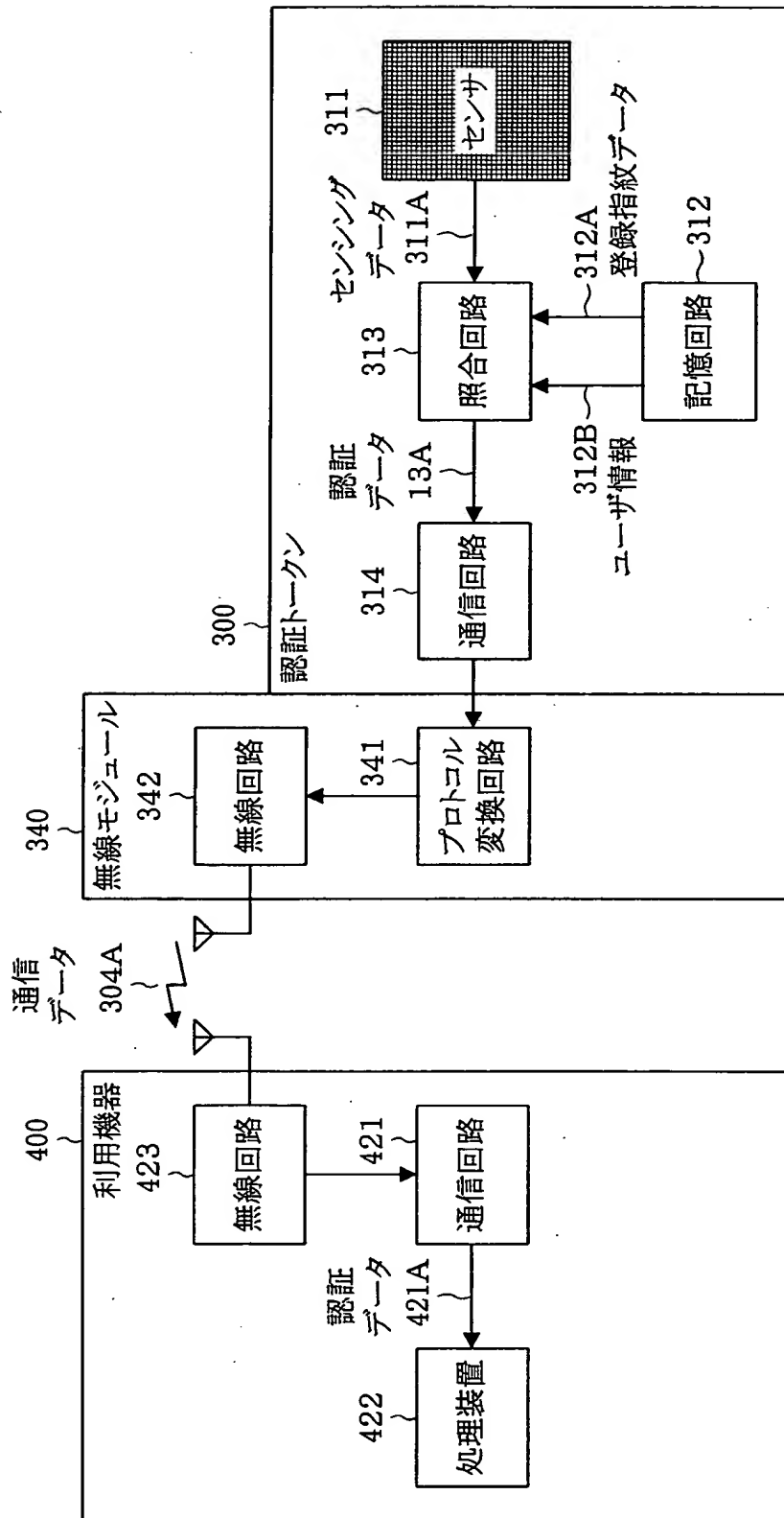
ユーザID
パスワード
照合結果
個人情報
⋮

【図 15】





【図 16】



【書類名】 要約書

【要約】

【課題】 利用者のコンサート会場等への入場の際にチケットのチェックを行う係員を必要とすることなくかつ利用者の速やかな入場を可能にするとともに、第三者による不正な入場を阻止する。

【解決手段】 コンサートのチケット購入時に利用者がその代金を支払うと、データベース102及び指紋認証トークン106にパスワードを記憶し、コンサート会場の入場時に指紋認証トークンにより利用者本人の確認を行い、利用者本人であることが認証されて指紋認証トークンから入場ゲート104近傍の無線／赤外線信号受信装置109へ無線または赤外線信号によるパスワードが送信されると、このパスワードを受信したゲートコントローラ103は、データベースのパスワードとの比較を行い双方のパスワードが一致すると入場ゲート104を開放する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社